A CHECKLIST FOR SUCCESS

# TOP 5 COMPLIANCE TIPS

PRACTICAL STEPS TO REDUCE INFORMATION MANAGEMENT RISK AND IMPROVE COMPLIANCE

**TO HELP YOUR COMPANY LOWER ITS RISK PROFILE AND BOOST AUDIT AND LITIGATION READINESS, WE'VE DEVELOPED A LIST OF THE TOP FIVE THINGS YOU CAN DO TODAY TO MAKE YOUR INFORMATION MANAGEMENT PRACTICES A KEY CONTRIBUTOR TO ONGOING COMPLIANCE.**

## 1. RETAIN, SECURE, DISPOSE

Knowing what to keep – for how long – and how to store it are challenges for many companies. And when it comes to compliance, a single misstep can have significant and costly consequences. But the fact remains that with all of the information you create and distribute each day, you must recognise what's critical and what's just "in the way." The best way to do this is to engage your company's legal counsel to develop a formal, defensible retention schedule that accounts for information in paper and digital formats. This policy must clearly outline what should be kept and for how long – and be enforceable across the business. Putting in the hard work today will pay off in the long run by mitigating the financial and reputation risk associated with issues such as failed audits or inadvertent disclosures of sensitive information.

## 2. DON'T FORGET ABOUT DESTRUCTION

Having a policy in place to securely destroy records after their useful lives is an important part of Records and Information Management (RIM) compliance. But what if a record marked for destruction is suddenly needed for discovery? If you can't put a quick stop to this process, you may find yourself subject to fines and other penalties related to the inadequate preservation of records. Given the ramifications of failing to produce the appropriate records during litigation, it's important that your RIM practice includes a formal destruction hold policy. And be sure to develop procedures – and leverage supporting technologies – that allow you to enforce the policy across the business. With this in place you'll be able to suspend the disposal of any paper or electronic record that is relevant to a pending investigation or audit.

## 3. HOLD ELECTRONIC RECORDS TO A HIGHER STANDARD

Because paper has been the norm for so long, it's likely that your retention and discovery processes are in place for these records. But what about electronic information? As more and more business is conducted electronically, your policies must also account for information in this format. Be sure that all electronic information, regardless of where it lives – PCs, servers, backup tapes, mobile devices, USB's and more – is included in your retention schedule. Clearly define what information is considered a record and develop policies and procedures to consistently and securely manage litigation holds and destruction when this information reaches the end of its retention period. In addition, ensure you have a clear process when it comes to eDiscovery and that you have a provider that can manage your data restoration requirements on these devices in a timely manner.

# TOP 5 COMPLIANCE TIPS

PRACTICAL STEPS TO REDUCE INFORMATION MANAGEMENT RISK
AND IMPROVE COMPLIANCE

## 4. PROVIDE START-TO-FINISH SECURITY

Protecting information at all times is a key to avoiding risk. But when you aren't sure when a record changes custodians, is put in a box or moved to tape media, keeping it secure for the long term can be quite the challenge. To solve this puzzle, make sure your workflows include an auditable chain-of-custody that documents every move a particular record makes. This way you'll always know where a record is at any given point in time. Documenting chain-of-custody in this way will help you ensure the ongoing safety of your most critical records and avoid the potential of an inadvertent breach in information security – and the resulting fines and penalties.

## 5. TAKE A PROGRAMMATIC APPROACH

While it's great to have a comprehensive set of RIM policies, these are only as strong as the people charged with enforcing, updating and communicating them across your company. And without the right amount of accountability, there may be critical lapses in your day-to-day activities that lead to the unauthorised disclosure or destruction of sensitive information.

To minimise the chances that this occurs, think about information management as a comprehensive program defined by policies and procedures managed by a specific individual – as well as a steering committee that can apply and enforce responsibilities across the business. Putting the right people and processes in place to audit the program will help you determine if it remains aligned with all pertinent regulations. Building accountability into your information management processes in this way will go a long way towards strengthening your company's compliance posture.

Today's regulatory landscape is evolving at an astonishing rate. So whether you're challenged to conform to certain regulations, or keep pace with industry mandates, the act of achieving – and maintaining – RIM compliance has become quite complicated.

**0861 476 668  |  IRONMOUNTAIN.CO.ZA**